MACQUARIE
University

COMP343 / ITEC643 – Week 2

Introduction to Number Theory

A / Prof Christophe Doche
Department of Computing

E6A 371 – christophe.doche@mq.edu.au

First Session 2017

Plan

Integer Representation

Euclidean Division

Prime Numbers and Factorisation

GCD

Modular Arithmetic

Birthday Paradox

Elliptic Curves

Integer Representation

Integer Representation

We normally represent integers in base 10

Example. 123456 stands for

$$1\times 10^5+2\times 10^4+3\times 10^3+4\times 10^2+5\times 10^1+6\times 10^0$$

Remark. This can be generalized to any fixed integer $b \geqslant 2$ called the radix or the base

Integer Representation

Take $b \geqslant 2$

Every integer $u > 0$ can be written in base b as

$$u = u_{n-1}b^{n-1} + \cdots + u_1 b + u_0$$

where $0 \leqslant u_i < b$, for all i

This expansion is denoted $(u_{n-1} \ldots u_0)_b$

Integer Representation

Remark. Another popular choice, especially in computing is $b = 2$ or $b = 2^k$

Hexadecimal notation corresponds to $b = 2^4$

We will use the `C` notation starting with 0x

What is the decimal value of `0xFFFF`?

Integer Representation

Properties.

Multiplying u by b^m shifts the digits of u to the left by introducing m zeroes at the end

$$(u_{n-1} \ldots u_0)_b \times b^m = (u_{n-1} \ldots u_0 \underbrace{0 \ldots 0}_{m \text{ times}})_b$$

Integer Representation

Properties.

Dividing u by b^m shifts the digits of u to the right by truncating the last m digits

$$\lfloor (u_{n-1} \ldots u_0)_b / b^m \rfloor = (u_{n-1} \ldots u_m)_b$$

Integer Representation

Consequence.

The Euclidean division of

$$u = (u_{n-1} \dots u_0)_b$$

by b^m satisfies

$$u = b^m q + r$$

with $\quad q = (u_{n-1} \dots u_m)_b$ and $r = (u_{m-1} \dots u_0)_b$

Euclidean

Division

Euclidean Division

Given $a, b \in \mathbb{Z}$, we can always write

$$a = bq + r \quad \text{with} \quad 0 \leqslant r < b$$

in a unique way, where q is the quotient and r is the remainder

We have $q = \lfloor a/b \rfloor$ and $r = a \bmod b$

Euclidean Division

Example. Let $a = 13$ and $b = 3$. We have

$$13 = 3 \times 4 + 1$$

Euclidean Division

Definition. We say that b divides a or that b is a divisor of a iff $a = bq$ and we write $b \mid a$

Examples.

7 is a divisor of 56.

We also say that 56 is a multiple of 7

$1 \mid n$, for all n

$n \mid 0$, for all n

PARI/GP

Useful commands

```
divrem
%
\
```

Prime Numbers
&
Factorisation

Prime Numbers

A prime number is an integer with exactly two divisors: 1 and itself

Facts.

- 1 is not prime
- 2 is the only prime that is even
- There are infinitely many prime numbers

Prime Numbers

Let p_k be the k-th prime number

It is possible to show that

$$p_k \sim k \log k$$

In other words

$$\frac{p_k}{k \log k} \to 1$$

when k tends to infinity

Factorisation

Factorisation consists in finding the prime factors of an integer

It is straightforward to multiply two primes

It is much more challenging to factor a large integer that is the product of two prime numbers

This asymmetry is used to design cryptoprimitives

Factorisation

Fundamental Theorem of Algebra.

Every integer $n > 1$ can be written in a unique way (up to a permutation of the factors) as a product of powers of prime numbers

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

where the α_i's are nonnegative integers

PARI/GP

Useful commands

```
isprime
prime
nextprime
randomprime
forprime
factor
```

GCD

Greatest Common Divisor

Given two integers $a > b$, $\gcd(a, b)$ is the largest integer d such that $d \mid a$ and $d \mid b$

It satisfies

1. $d \mid a$ and $d \mid b$
2. whenever $c \mid a$ and $c \mid b$, then $c \mid d$

Greatest Common Divisor

Bezout relation.

Let $d = \gcd(a, b)$

There are two integers u and v such that

$$au + bv = d$$

Greatest Common Divisor

We can compute $\gcd(a, b)$ using that if $a = bq + r$ then

$$\gcd(a, b) = \gcd(b, r)$$

Greatest Common Divisor

Euclid's Algorithm.

Let $a = bq + r$ and let us us prove that

$$\gcd(a, b) = \gcd(b, r)$$

We show that

$$\gcd(a, b) \mid \gcd(b, r) \quad \text{and} \quad \gcd(b, r) \mid \gcd(a, b)$$

Greatest Common Divisor

Algorithm. Euclid GCD

INPUT: Two integers a and b such that $a > b$.
OUTPUT: The integer d such that $d = \gcd(a, b)$.

```
repeat
        r ← a mod b
        a ← b and b ← r
until r = 0
d ← a
return d
```

Greatest Common Divisor

Example. Let us compute the gcd of 91 and 35

$$\begin{aligned} 91 &= 35 \times 2 + 21 \\ 35 &= 21 + 14 \\ 21 &= 14 + 7 \\ 14 &= 7 \times 2 + 0 \end{aligned}$$

So

$$\gcd(91, 35) = \gcd(35, 21) = \cdots = \gcd(7, 0) = 7$$

Greatest Common Divisor

Algorithm. Euclid GCD (recursive version)

INPUT: Two integers a and b such that $a > b$.
OUTPUT: The integer d such that $d = \gcd(a, b)$.

1. $d \leftarrow a$
2. **if** $b \neq 0$ **then**
3. $\quad r \leftarrow a \bmod b$
4. $\quad d \leftarrow \gcd(b, r)$
5. **return** d

Least Common Multiple

$d = \text{lcm}(a, b)$ is the smallest non-negative integer divisible by both a and b.

It satisfies

1. $a \mid d$ and $b \mid d$
2. whenever $a \mid c$ and $b \mid c$, then $d \mid c$
3. $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$

Greatest Common Divisor

Euler's Totient Function.

Definition. Two integers a and b are said to be coprime iff $\gcd(a, b) = 1$

Definition. The Euler's totient function of $n > 0$ denoted by $\varphi(n)$ is the number of integers in $[1, n]$ coprime with n

Example. We have $\varphi(15) = 8$

Indeed, $1, 2, 4, 7, 8, 11, 13, 14$ are coprime with 15

Greatest Common Divisor

Properties.

- If p is a prime number, then $\varphi(p) = p - 1$

- If p and q are distinct prime numbers then

$$\varphi(pq) = (p-1)(q-1)$$

- More generally, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

PARI/GP

Useful commands

```
gcd
bezout
lcm
eulerphi
```

Modular

Arithmetic

Modular Arithmetic

Congruence.

Definition. Let n be a positive integer

We say that a is congruent to b mod n iff $n \mid (b - a)$

It is denoted by $a = b \pmod{n}$

Example. 2 and 16 are congruent modulo 14

Modular Arithmetic

Class.

Definition. A class modulo n is a set containing all the integers which are congruent mod n

Example. Let $n = 14$. The class of 2 modulo 14 denoted by $\overline{2}$ or $[2]_{14}$ is the set

$$\{\ldots, -26, -12, 2, 16, 30, \ldots\}$$

Modular Arithmetic

Operations modulo n.

We can define an addition and a multipication modulo n

Namely, we have $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \times \overline{b} = \overline{a \times b}$

Modular Arithmetic

$$\begin{array}{|cccccr|}
\hline
5 & \times & 1 & = & & \pmod{11} \\
5 & \times & 2 & = & & \pmod{11} \\
5 & \times & 3 & = & & \pmod{11} \\
5 & \times & 4 & = & & \pmod{11} \\
5 & \times & 5 & = & & \pmod{11} \\
5 & \times & 6 & = & & \pmod{11} \\
5 & \times & 7 & = & & \pmod{11} \\
5 & \times & 8 & = & & \pmod{11} \\
5 & \times & 9 & = & & \pmod{11} \\
5 & \times & 10 & = & & \pmod{11} \\
5 & \times & 11 & = & & \pmod{11} \\
\hline
\end{array}$$

Modular Arithmetic

$$
\boxed{\begin{array}{cccccc}
5 & \times & 1 & = & 5 & \pmod{11} \\
5 & \times & 2 & = & 10 & \pmod{11} \\
5 & \times & 3 & = & 4 & \pmod{11} \\
5 & \times & 4 & = & 9 & \pmod{11} \\
5 & \times & 5 & = & 3 & \pmod{11} \\
5 & \times & 6 & = & 8 & \pmod{11} \\
5 & \times & 7 & = & 2 & \pmod{11} \\
5 & \times & 8 & = & 7 & \pmod{11} \\
5 & \times & 9 & = & 1 & \pmod{11} \\
5 & \times & 10 & = & 6 & \pmod{11} \\
5 & \times & 11 & = & 0 & \pmod{11}
\end{array}}
$$

Modular Arithmetic

$$
\boxed{\begin{array}{llllr}
4 & \times & 1 & = & \pmod{12} \\
4 & \times & 2 & = & \pmod{12} \\
4 & \times & 3 & = & \pmod{12} \\
4 & \times & 4 & = & \pmod{12} \\
4 & \times & 5 & = & \pmod{12} \\
4 & \times & 6 & = & \pmod{12} \\
4 & \times & 7 & = & \pmod{12} \\
4 & \times & 8 & = & \pmod{12} \\
4 & \times & 9 & = & \pmod{12} \\
4 & \times & 10 & = & \pmod{12} \\
4 & \times & 11 & = & \pmod{12} \\
4 & \times & 12 & = & \pmod{12}
\end{array}}
$$

Modular Arithmetic

$$\boxed{\begin{aligned}
4 &\times 1 = 4 \pmod{12}\\
4 &\times 2 = 8 \pmod{12}\\
4 &\times 3 = 0 \pmod{12}\\
4 &\times 4 = 4 \pmod{12}\\
4 &\times 5 = 8 \pmod{12}\\
4 &\times 6 = 0 \pmod{12}\\
4 &\times 7 = 4 \pmod{12}\\
4 &\times 8 = 8 \pmod{12}\\
4 &\times 9 = 0 \pmod{12}\\
4 &\times 10 = 4 \pmod{12}\\
4 &\times 11 = 8 \pmod{12}\\
4 &\times 12 = 0 \pmod{12}
\end{aligned}}$$

Modular Arithmetic

Inverse.

Any nonzero element has an inverse modulo a prime number p

This inverse can be found using Bezout relation

$$au + bp = 1$$

Which implies that

$$au = 1 \pmod{p}$$

Modular Arithmetic

Inverse.

Modulo a composite number any element a that is coprime with n has an inverse modulo n

Again, this inverse can be found using Bezout relation

$$au + bn = 1$$

Which implies that

$$au = 1 \pmod{n}$$

Modular Arithmetic

Exponentiation.

To compute x^k modulo n one could compute x^k and then reduce the final result modulo n

It is smart to reduce the intermediate computations modulo n

Also, we use a fast exponentiation technique called square and multiply

Modular Arithmetic

Algorithm. Square and multiply

INPUT: An element x and an integer $k = (k_{\ell-1} \ldots k_0)_2$.
OUTPUT: The element x^k.

1. $t \leftarrow 1$
2. **for** $i = \ell - 1$ **downto** 0 **do**
3. $\quad t \leftarrow t^2$
4. $\quad$ **if** $k_i = 1$ **then** $t \leftarrow t \times x$
5. **return** t

Modular Arithmetic

Example. Let us compute x^{21}

$$21 = (10101)_2$$

t	$1,$	$1,$	$x,$	$x^2,$	$x^4,$	$x^5,$	$x^{10},$	$x^{20},$	x^{21}
i		4		3	2		1	0	

Modular Arithmetic

Fermat's Theorem.

Let p be a prime number, then for every $a \in \mathbb{Z}$ coprime with p we have

$$a^{p-1} = 1 \pmod{p}$$

Modular Arithmetic

Euler's Theorem.

Let N and a be integers such that $\gcd(a, N) = 1$ then

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

where $\varphi(N)$ is the Euler's totient function

Modular Arithmetic

Fermat test.

Based on Fermat's theorem, we deduce Fermat compositeness test

1. choose a random $a \in [1, N-1]$
2. **if** $a^{N-1} \not\equiv 1 \pmod{N}$ return that N is composite
3. **else** return that N is prime

Modular Arithmetic

Fast exponentiation makes this test very efficient

However, even if N is composite, there can be some values a such that

$$a^{N-1} = 1 \pmod{N}$$

Modular Arithmetic

Such a value a is called a false witness

It tells us that N is likely to be prime but it lies!

Example. Let $N = 4087$ and

We have $841^{N-1} = 1 \pmod N$

Also, $1905^{N-1} = 1 \pmod N$

These values suggest that N is prime...

PARI/GP

Useful commands

```
Mod
%
+
-
*
/
^
lift
```

Birthday

Paradox

Birthday Paradox

Take a group of n people

Question. What is the probability that at least 2 people in the group have the same birthday?

Birthday Paradox

Take a group of n people

Question. What is the probability that at least 2 people in the group have the same birthday?

Answer. It depends on n

If there are only 2 people in the group, i.e. $n = 2$ the probability is close to 0

If $n > 365$ this probability is 1

Birthday Paradox

Now, what is the order of magnitude of n so that the probability to have 2 people with the same birthday is equal to $1/2$

In other words, how large should be the group to have a reasonable chance to find 2 people with the same birthday

Is it $n = 200, 150, 100, 50$ or 20?

Birthday Paradox

In fact n should be approximately equal to 23

This is surprisingly low, hence the term paradox

You don't believe it?

Ok, let us simulate it!

Birthday Paradox

Let $B = 365$ and let us consider lists of length n with elements $\leqslant B$

If a list has at least 2 elements that are the same, we have a match (or a collision)

Then generate a (very) large number of lists at random

For each list check if it contains a match, and deduce an approximation of the probability

Birthday Paradox

Consequence.

If we consider a list of length $O(\sqrt{B})$, we can reasonably expect that this list contains 2 identical elements

Another formulation:

If we draw elements at random from $[1, B]$, we can expect a match after $O(\sqrt{B})$ draws

Birthday Paradox

Pollard's rho method.

This factoring method was introduced in 1975 by Pollard

It was refined by Brent to factor the eighth Fermat number $F_8 = 2^{2^8} + 1$ in 1980

This method relies on the birthday paradox

Birthday Paradox

Algorithm. Pollard's rho

INPUT: A positive integer N.
OUTPUT: A nontrivial factor of N or a failure message.

$x \leftarrow 2, y \leftarrow 2$
while true do
    $x \leftarrow x^2+1 \bmod N$ and $y \leftarrow y^4+2y^2+2 \bmod N$
    $g \leftarrow \gcd(y-x, N)$
    if $g > 1$ **then break**
if $g = N$ **then** the algorithm fails **else return** g

Elliptic

Curves

Elliptic Curves

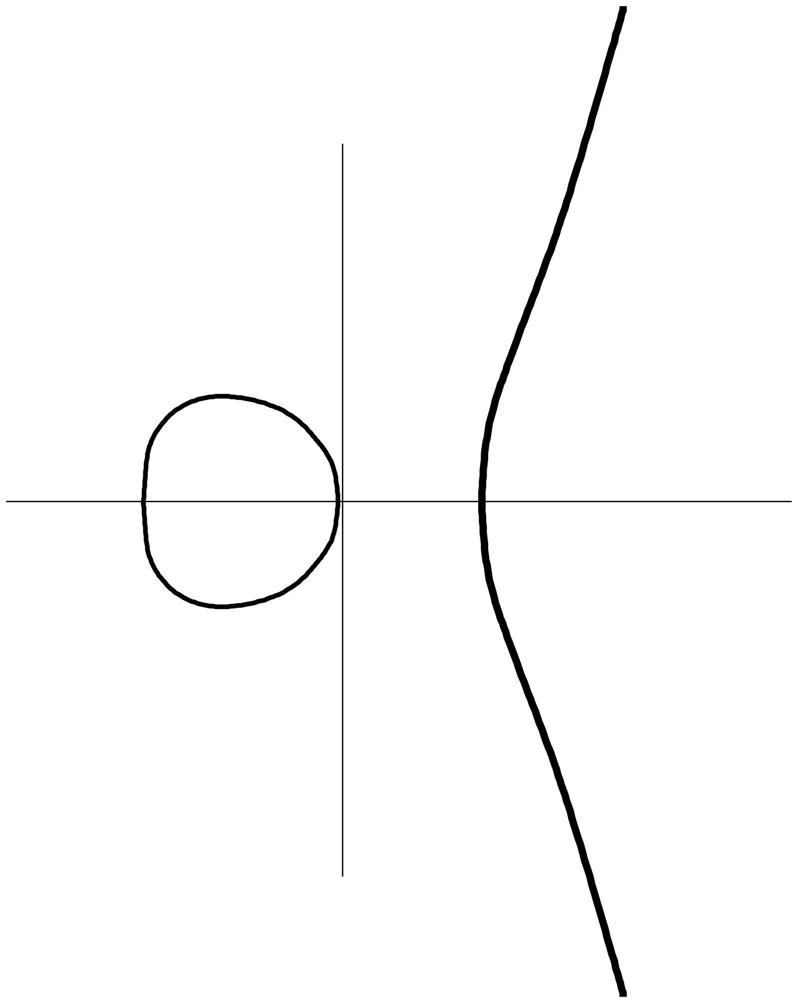
Definition. An elliptic curve defined modulo p is given by an equation of the form

$$y^2 = x^3 + ax + b \pmod{p}$$

with a and b integers such that

$$4a^3 + 27b^2 \neq 0 \pmod{p}$$

Elliptic Curves



Elliptic curve $y^2 = x^3 - x$ defined over $\mathbb{R}$

Elliptic Curves

Example. Take $p = 2017$ and E defined modulo p by the equation

$$E : y^2 = x^3 + 2x + 1$$

The point $P = [1, 2]$ is on the curve as

$$2^2 = 1 + 2 + 1$$

The point $[51, 866]$ is also on the curve, as

$$866^2 = 51^3 + 2 \times 51 + 1 \pmod{p}$$

Elliptic Curves

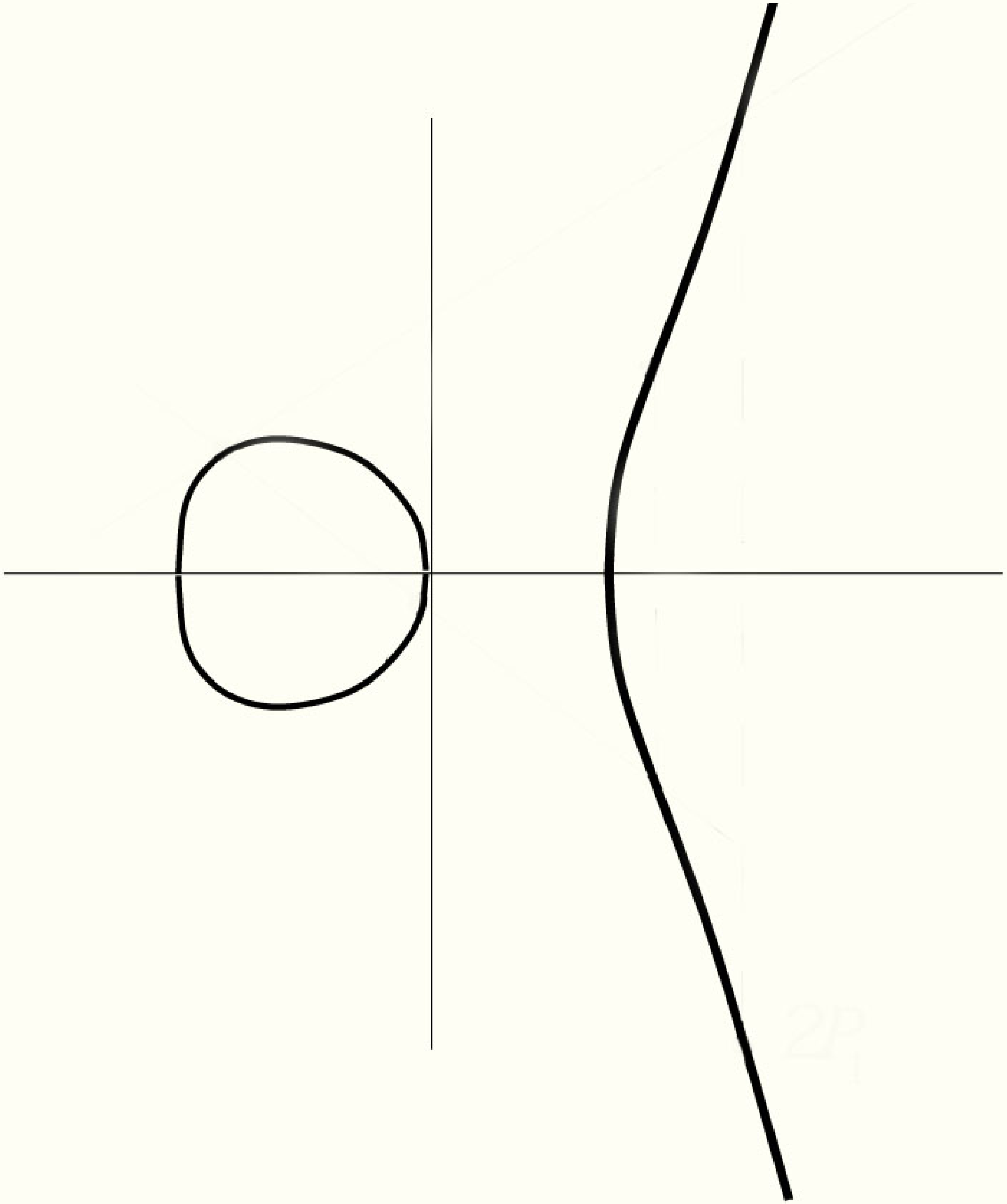
There is a recipe to add points on the curve

Let $P_1 = [x_1, y_1]$ and $P_2 = [x_2, y_2]$ on E

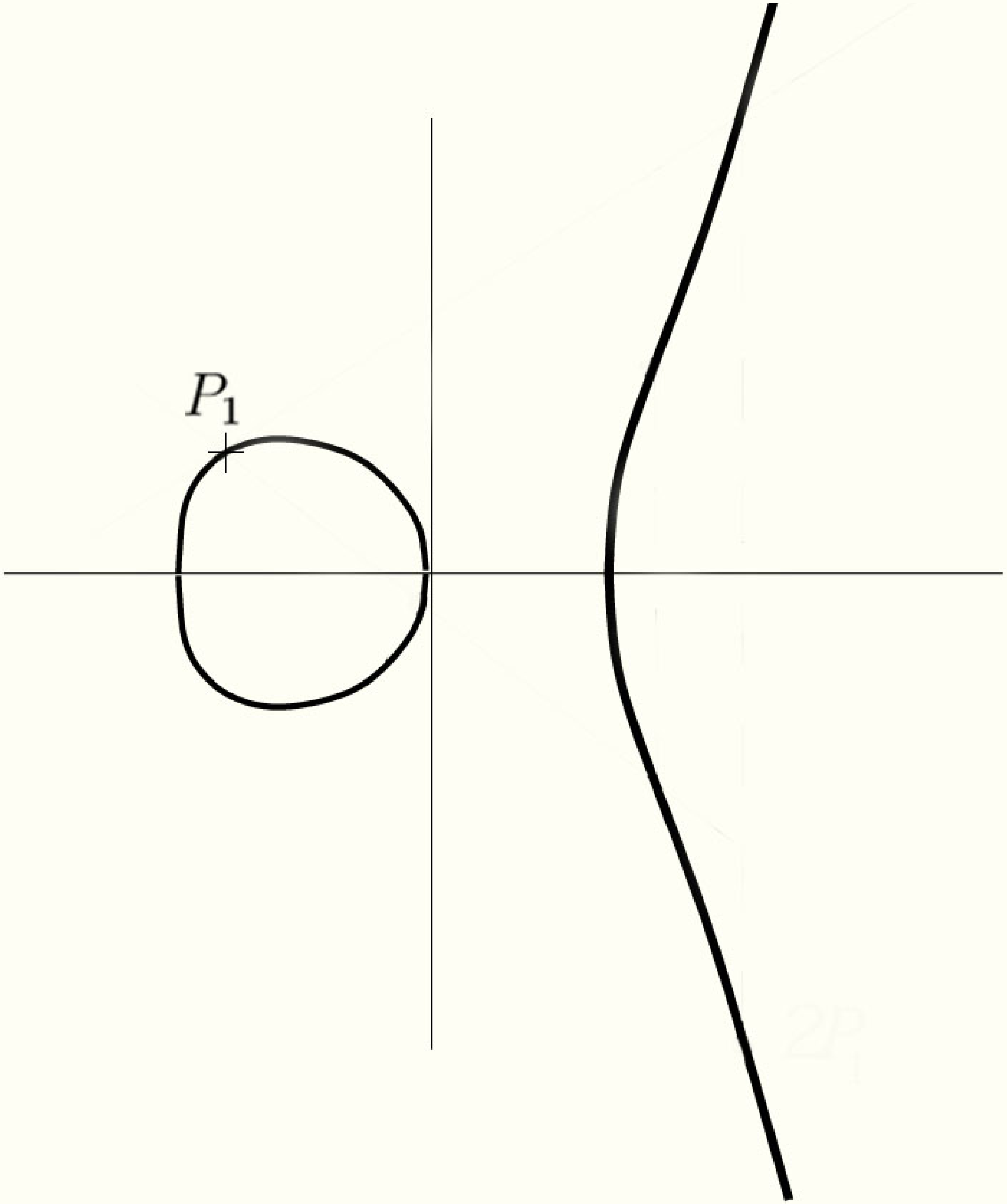
It is possible to associate to P_1 and P_2 another point, also on the curve, denoted by P_1+P_2

We proceed as follows

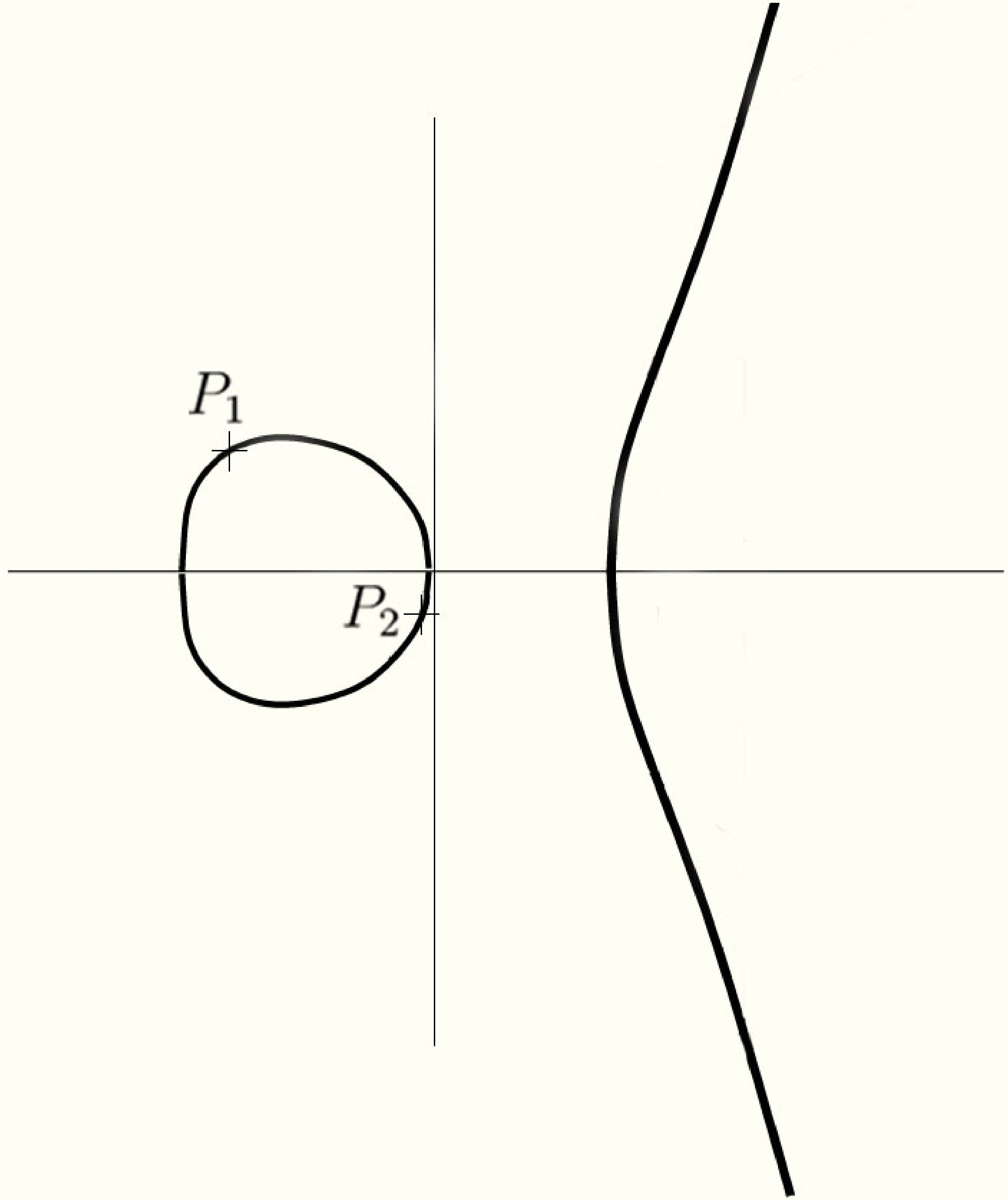
Addition of two points P_1 and P_2



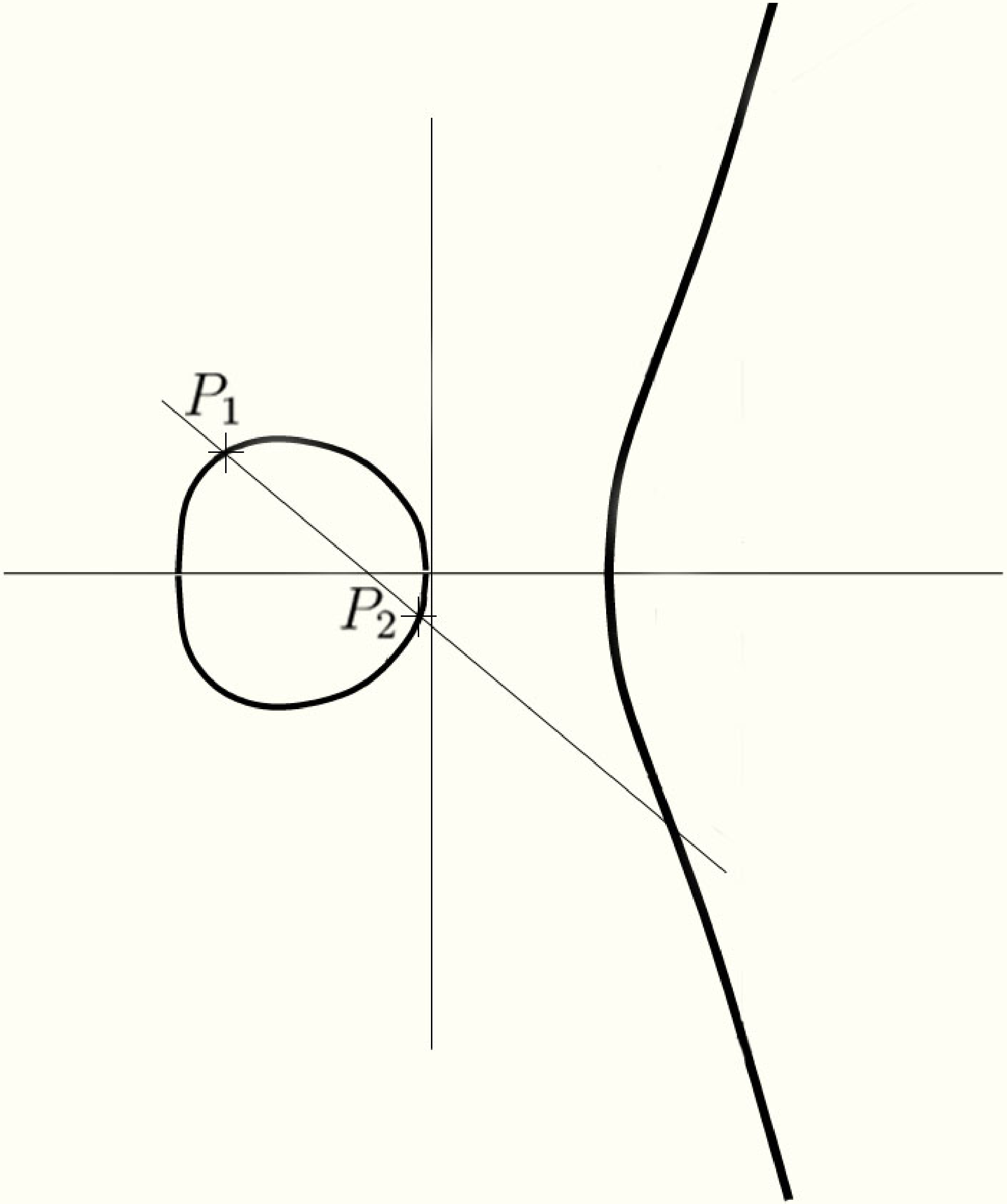
Addition of two points P_1 and P_2



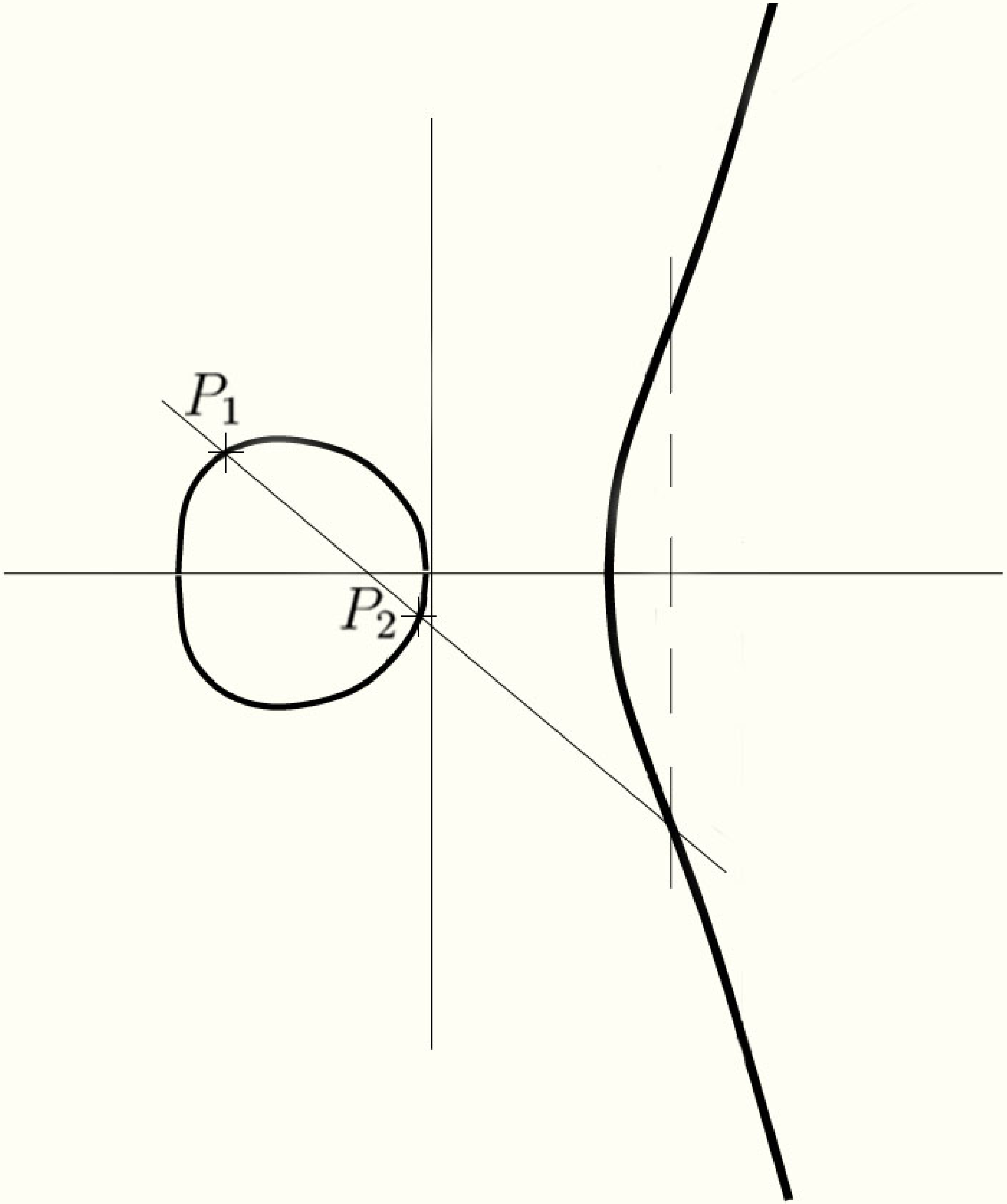
Addition of two points P_1 and P_2



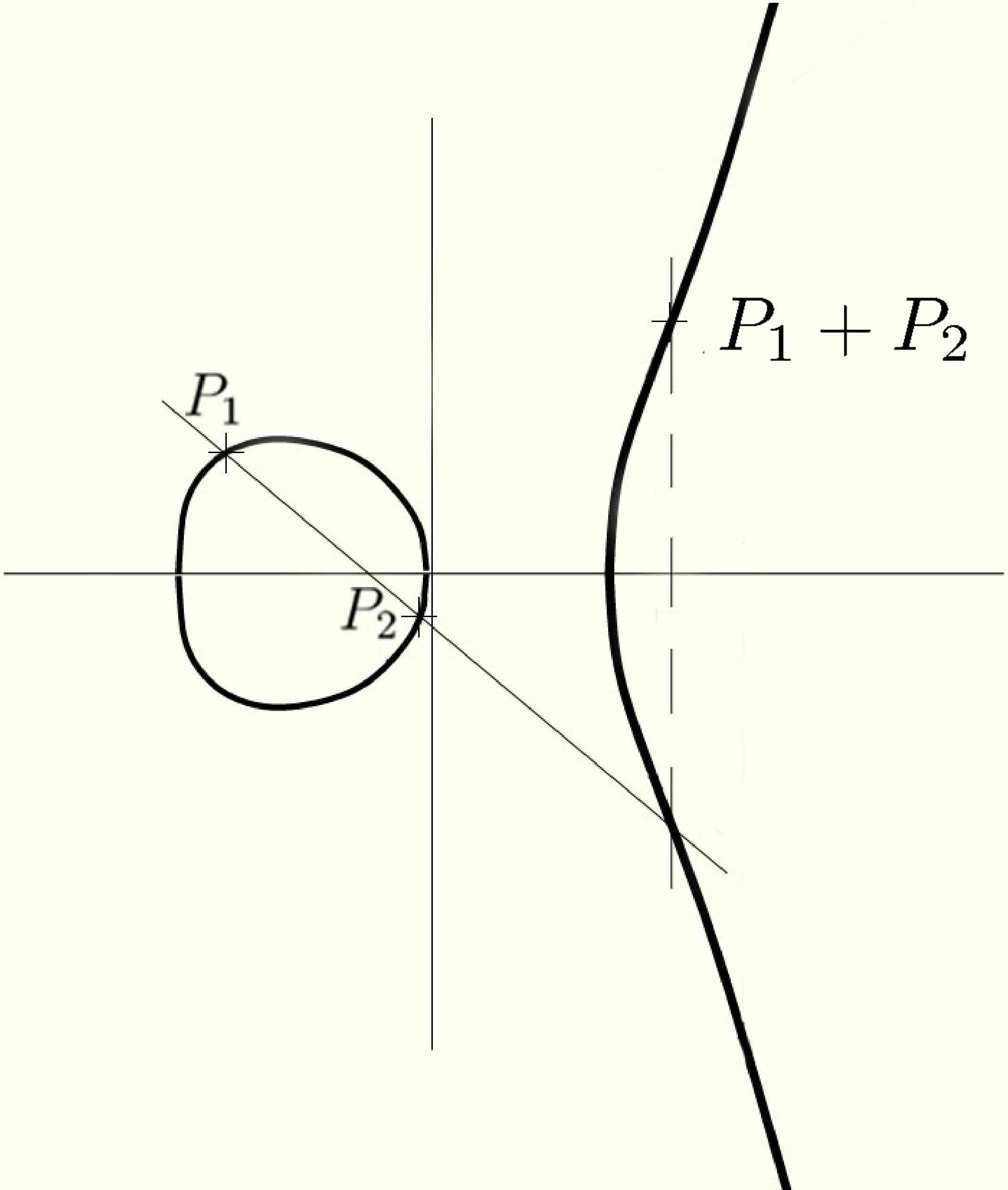
Addition of two points P_1 and P_2



Addition of two points P_1 and P_2



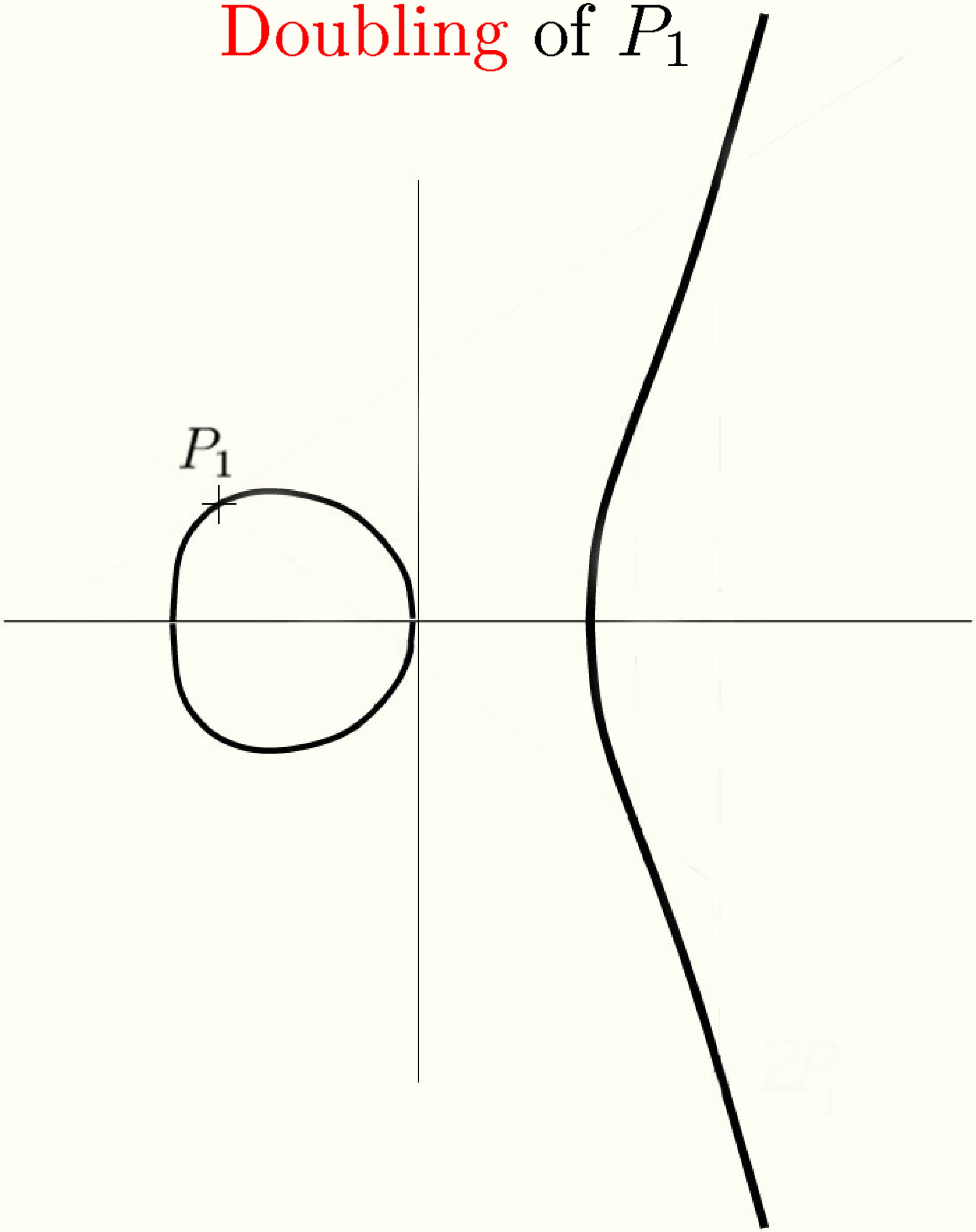
Addition of two points P_1 and P_2



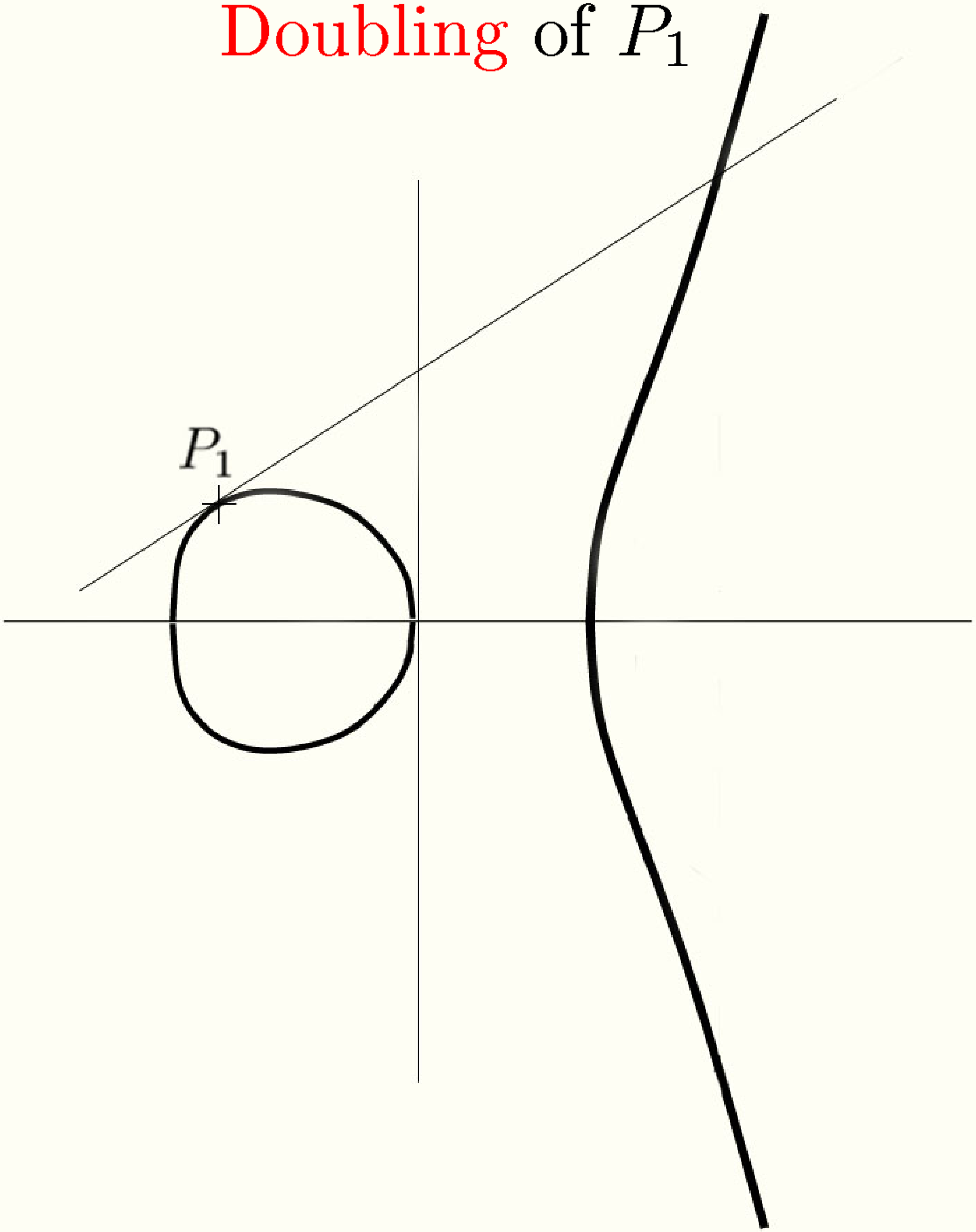
Elliptic Curves

To add P_1 to itself, we need to modify the approach a bit

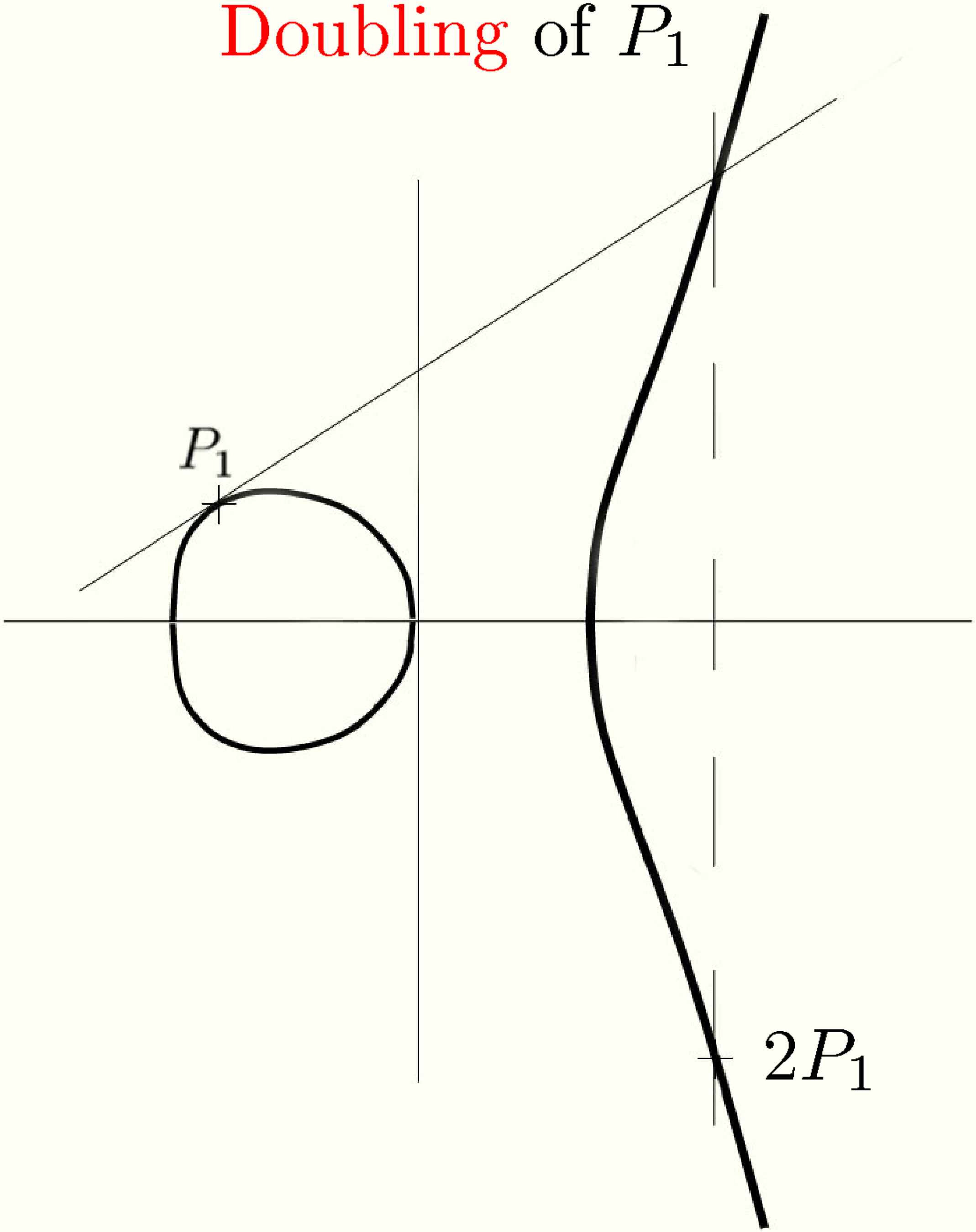
Doubling of P_1



Doubling of P_1



Doubling of P_1

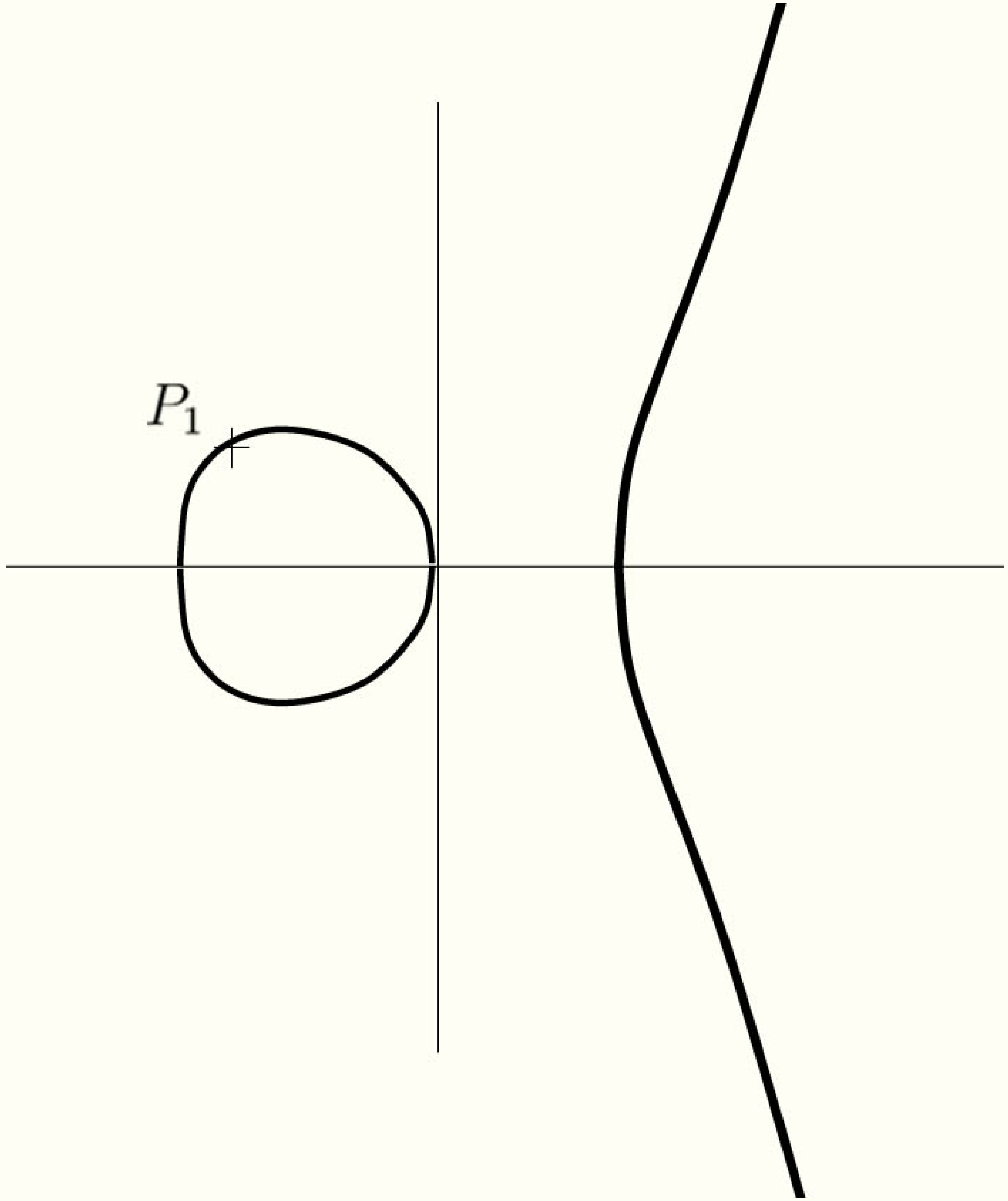


Elliptic Curves

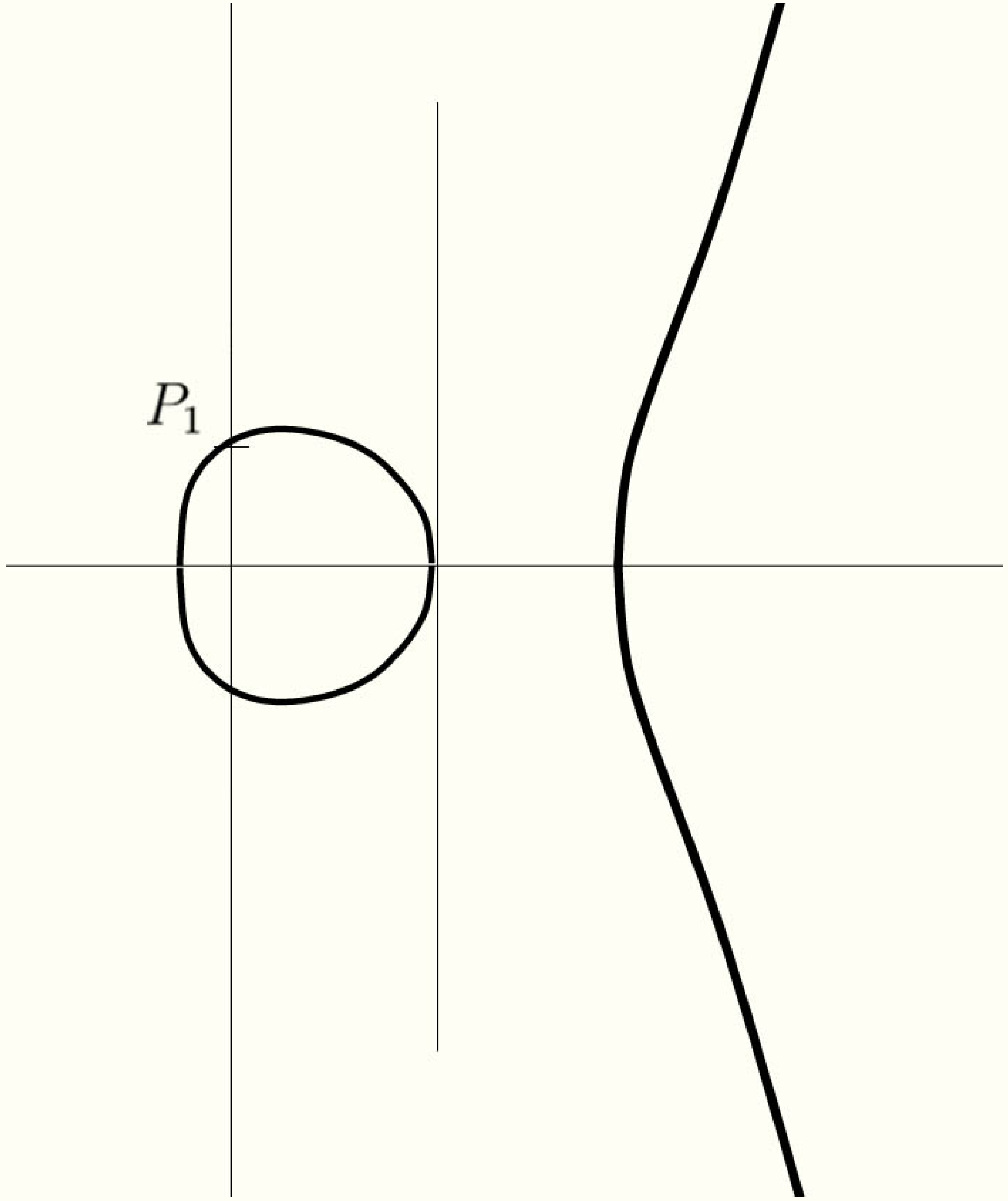
You may ask yourself what is the neutral element for this addition law?

Which element is going to leave any point unchanged?

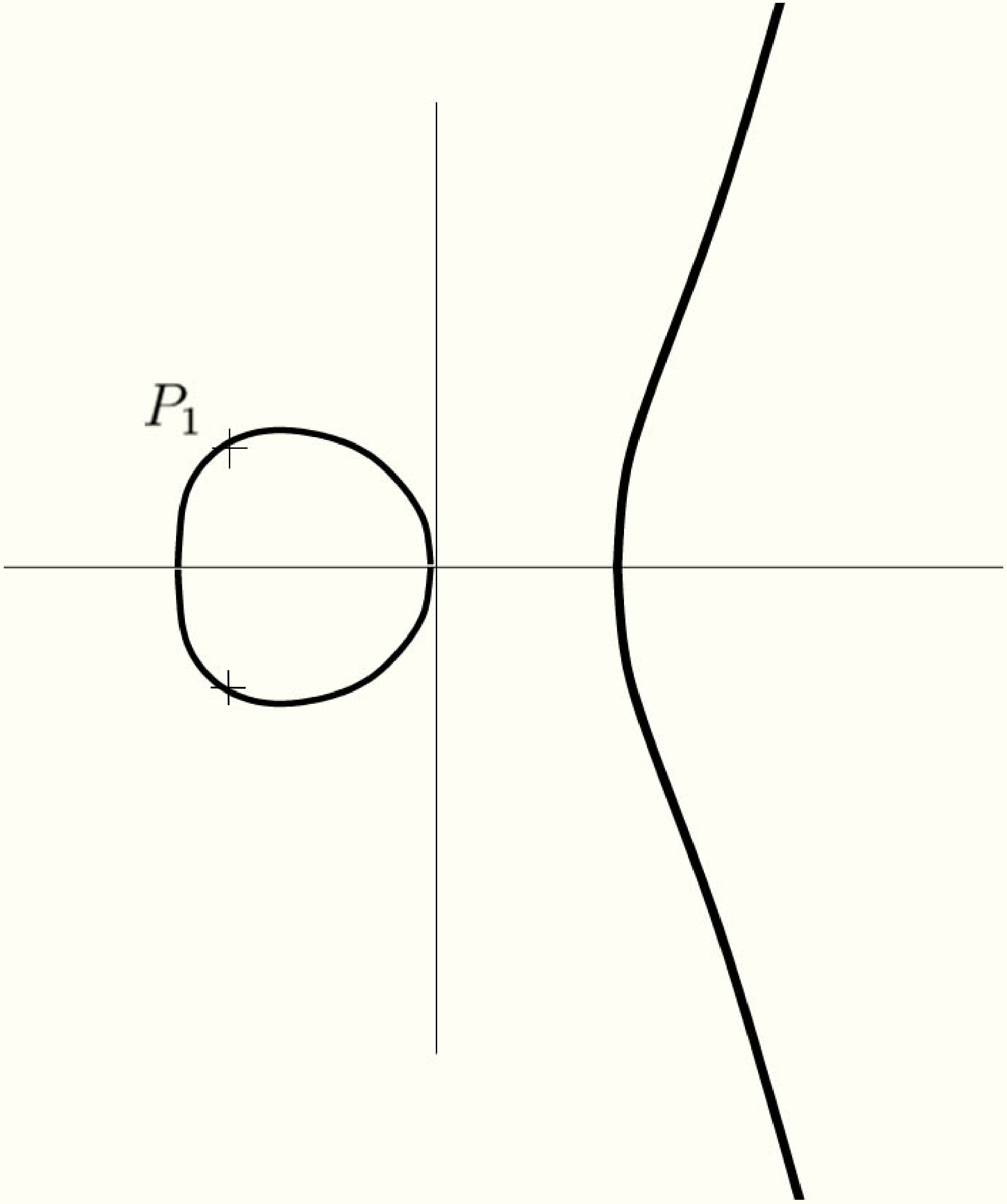
Addition of P_1 to the point at infinity



Addition of P_1 to the point at infinity

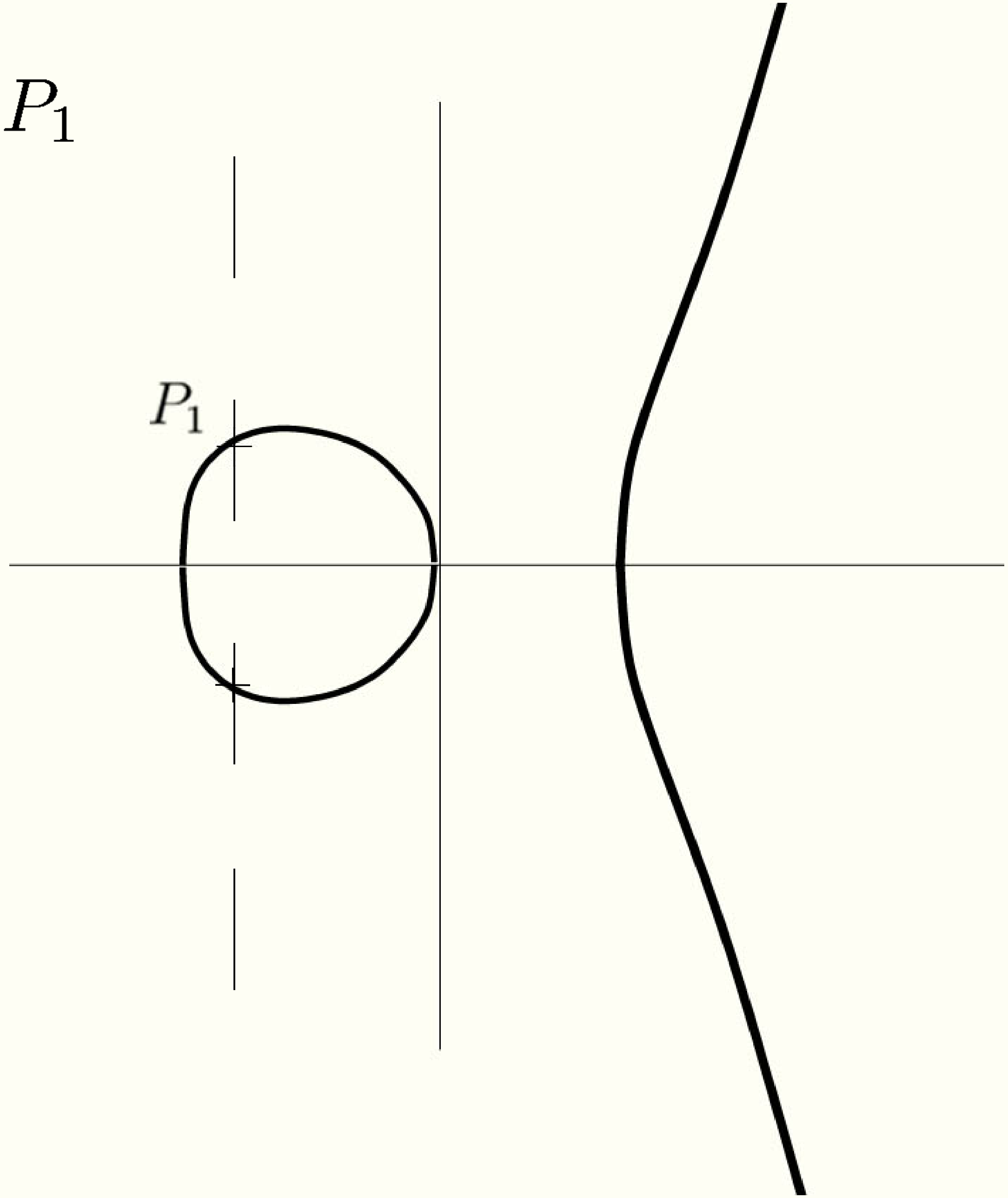


Addition of P_1 to the point at infinity



Addition of P_1 to the point at infinity

$$P_1 + [0] = P_1$$



Elliptic Curves

An affine point is a point of the form $[x_1, y_1]$

The point at infinity is a special point, that cannot be represented as $[x_1, y_1]$

It is denoted by $[0]$

Elliptic Curves

From the previous diagrams, it is possible to derive formulas to add or double any point on the curve

Elliptic Curves

$P_1 + P_2 = [x_3, y_3]$

where $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$

and λ is the slope defined by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2 \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & \text{otherwise} \end{cases}$$

Elliptic Curves

The arithmetic on the curve

$$E : y^2 = x^3 + ax + b$$

modulo a large prime p is given by the same formulas as for the real case

Elliptic Curves

Definition.

All the points on an ellitpic curve E together with the point at infinity form a finite set

This set endowed with the addition law that we defined previously forms the group of rational points of E

Elliptic Curves

Scalar multiplication.

Definition. Given an integer n and a point P on the curve, the scalar multiplication is the operation

$$nP = \underbrace{P + \cdots + P}_{n \text{ times}}$$

Of course for any $n \in \mathbb{Z}$, then nP is again on the curve

Elliptic Curves

Order of a Point.

Definition. The order of a point P is the smallest positive integer k such that $kP = [0]$

Elliptic Curves

Discrete Logarithm Problem.

Given an integer n and point P on E, it is straightforward to compute $Q = nP$

Given, P and Q, it is much more challenging to retrieve n such that $Q = nP$

This asymmetry can again be used to implement cryptoprimitives

PARI/GP

Useful commands

```
ellinit
ellisoncurve
ellorder
ellordinate
elladd
ellsub
ellpow
```